**Ssh登录**

Ssh是建立在应用层和传输层的安全协议，专门为远程登录回话和其他网络服务提供安全性。利用ssh可以有效的防止远程管理中的信息泄露问题，同时ssh传输的数据是经过压缩的，可以加快传输速度。

1、启动sshd服务。Centos默认已经安装了ssh，而且该服务默认是启动的

|  |
| --- |
| [root@localhost wj]# **rpm -qa | grep ssh**  libssh2-1.4.2-1.el6.i686  openssh-askpass-5.3p1-94.el6.i686  openssh-server-5.3p1-94.el6.i686  openssh-clients-5.3p1-94.el6.i686  openssh-5.3p1-94.el6.i686  [root@localhost wj]# **service sshd status**  openssh-daemon (pid 1634) 正在运行...  [root@localhost wj]# |

2、测试登录

|  |
| --- |
| [root@localhost wj]# **ssh root@192.168.0.119**  The authenticity of host '192.168.0.119 (192.168.0.119)' can't be established.  RSA key fingerprint is 36:20:c9:ab:88:1f:47:74:1b:f1:d7:47:55:e0:14:7c.  Are you sure you want to continue connecting (yes/no)? yes  Warning: Permanently added '192.168.0.119' (RSA) to the list of known hosts.  **root@192.168.0.119's password:**  Last login: Fri Aug 10 14:57:45 2018  **already login**  [root@localhost ~]# **exit**  logout  Connection to 192.168.0.119 closed. |

3、禁止root登录

root用户在Linux系统中拥有最高的权利，如果用root用户登录就意味着增大了系统的风险。Ssh默认可以使用root登录，为了安全考虑，我们可以禁止root登录。

1）修改配置文件“/etc/ssh/sshd\_config”，找到“permitRootLogin”将其改为no

|  |
| --- |
| [root@localhost wj]# **gedit /etc/ssh/sshd\_config**  **PermitRootLogin no //这里默认是yes，而且已经被注释掉了。取消注释，改为no**  [root@localhost wj]# **service sshd restart //重启服务**  停止 sshd： [确定]  正在启动 sshd： [确定]  [root@localhost wj]# |

2）测试，使用root登录，可以看到没有权利

|  |
| --- |
| [root@localhost wj]# **ssh root@192.168.0.119**  **root@192.168.0.119's password:**  **Permission denied, please try again.** |

4、设置指定用户登录

有时候为了降低系统风险，我们还会设置指定的用户登录，而其他用户登录就会拒绝。

1）修改配置文件“/etc/ssh/sshd\_config”，在最后追加

|  |
| --- |
| [root@localhost wj]# **gedit /etc/ssh/sshd\_config**  **AllowUsers david //允许david登录**  [root@localhost wj]# **service sshd restart //重启服务**  停止 sshd： [确定]  正在启动 sshd： [确定]  [root@localhost wj]# |

2）测试，分别使用david和weijie两个用户登录，其中weijie会登录失败

|  |
| --- |
| [root@localhost wj]# **ssh weijie@192.168.0.119**  **weijie@192.168.0.119's password:**  **Permission denied, please try again.**  [root@localhost wj]# **ssh david@192.168.0.119**  **david@192.168.0.119's password:**  **Last login: Wed Aug 15 17:12:59 2018 from 192.168.0.112**  **already login** |

Copyright@david zhytwj2018@163.com